UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/606,161	06/25/2003	Sylvie Wuidart	00RO36654290	5008

27975 7590 04/13/2007

ALLEN, DYER, DOPPELT, MILBRATH & GILCHRIST P.A.
1401 CITRUS CENTER 255 SOUTH ORANGE AVENUE
P.O. BOX 3791
ORLANDO, FL 32802-3791

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/606,161	WUIDART, SYLVIE	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 February 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *11-22* is/are allowed.

6)☒ Claim(s) *1,6-9,23 and 25-31* is/are rejected.

7)☒ Claim(s) *5,10,24 and 32* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 June 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 2/9/2007 was received and considered.

2. Claims 1-32 are pending.

Response to Arguments

3. Applicant's arguments with respect to claims 1-32 have been considered but are moot in view of the new ground(s) of rejection. However, several pertinent arguments are addressed below.

4. Applicant's response (§III) argues that ON lacks different electrical paths. However, as explained below, transistors, by definition, react by either turning on or off based on input voltage levels, creating different electrical paths, and hence creating the proper logic level at output. Therefore, by receiving different inputs, different paths are taken to perform the same logical function (NOR).

5. Applicant's response (§III) argues that the 3-input NOR gate performs two different functions according to the selection signal. However, it is maintained that the circuit performs a NOR function, a fact that remains constant throughout operation. The circuit performs the NOR function in two different ways depending on the selection signal. The breadth of applicant's claim is such that circuit need only perform a logic function in two different ways; there are no limitations on what the logic function can entail, i.e. the breadth of a logic function. For instance, two different calculators would both perform, for instance the function of addition. Regardless of the fact that one may perform addition using a carry lookahead adder and the other a basic binary adder, they both perform the logic function of addition.

6. Applicant's response (§IV) argues that NS lacks different electrical paths. However, as explained below, transistors, by definition, react by either turning on or off based on input voltage levels, creating different electrical paths, and hence creating the proper logic level at output. Therefore, by receiving different inputs, different paths are taken to perform the same logical function (multiplexing). The Examiner maintains that the circuit performs a multiplexing function throughout operation. The circuit performs the multiplexing function in two different ways depending on the selection signal.

Claim Rejections - 35 USC § 112

7. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

8. Claims 6-9 & 25-31 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. Regarding claim 6, the limitation "said at least one logic gate" lacks sufficient antecedent basis. Claims 7-9 are rejected based on their dependence upon a rejected claim under this section.

b. Regarding claim 25, the claim is directed to a method, and it is unclear what effect, if any, lines 2-9 of the claim have on limiting the claim. Claim 26 is rejected based on its dependence upon a rejected claim under this section.

c. Regarding claim 27, the limitation "wherein the at least one logic block" lacks sufficient antecedent basis.

d. Regarding claim 28, the limitation "wherein the at least one logic block" lacks sufficient antecedent basis. Claims 29-31 are rejected based on their dependence upon a rejected claim under this section.

Claim Rejections - 35 USC § 102

9. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

10. Claim 1 is rejected under 35 U.S.C. 102(a) as being anticipated by MC14001B Series CMOS gates, described in "MC14001B Series B-Suffix Series CMOS Gates" by ON Semiconductor (**ON**).

Regarding claim 1, ON discloses a logic circuit (MC14025B Triple 3-Input NOR gate) for performing a logic function (NOR logic function), and having N (2) data inputs and M (1) data outputs, N being at least equal to 2 and M being at least equal to 1 (p. 2), the logic circuit comprising different logic gates or different transistors (p. 5, "MC14025B") for performing the logic function (NOR, p. 2) in at least two different ways (see table below, for example pin 1 high versus pin 1 low) corresponding to different data paths or different electrical paths through the different logic dates or different transistors (transistors, by definition, react by either turning on or off based on input voltage levels, creating different electrical paths, and hence creating the proper logic level at output), the way in which the logic function is performed being based upon

a value of a function selection signal (pin 1, p. 2) such that for identical data received at the N data inputs (pins 2 and 8, see p. 2 & p. 5, "MC14025B") and for different values of the function selection signal (pin 1), at least one of polarities of certain internal nodes of the logic circuit are not identical and current consumption of the logic circuit is not identical (see table and explanation below). As per the table below, and by the definition of the gate shown, if the function selection signal is a logic "0", an input of Pin 2 = "0" and Pin 3 = "0" yields an output Pin 9 = "1". Upon a different value of the function selection signal, Pin 1 = "1" with the identical inputs, the output, Pin 9 = "0". Therefore, the polarities of internal nodes of the circuit are not identical. Further, current consumption of the logic circuit is not identical (see table "Electrical Characteristics" on p. 3, where for a reference voltage constant, the output current is, for example, -3mA for a high output and the output current is 0.64mA.

Pin 1 (function selection)	Pin 2 (input 1)	Pin 3 (input 2)	Pin 9 (output)
0	0	0	1
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	0

11. Claim 1 is rejected under 35 U.S.C. 102(b) as being anticipated by the Quad 2-Line to 1-Line Data Selectors/Multiplexers, described in "Quad 2-Line to 1-Line Data Selectors/Multiplexers" by National Semiconductor (**NS**).

Regarding claim 1, NS discloses a logic circuit (p. 1) for performing a logic function (multiplexing, p. 1), and having at least N (2) data inputs and M (1) data outputs, N being at least equal to 2 and M being at least equal to 1 (p. 1), the logic circuit comprising different logic gates or different transistors ("Logic Diagrams", p. 4) for performing the logic function in at least two different ways (see "Function Table", p. 1 and elaboration of same described below) corresponding to different data paths or different electrical paths through the different logic gates or different transistors (logic gates, which are made of transistors, by definition, react by either turning on or off based on input voltage levels, creating different electrical paths, and hence creating the proper logic level at output), the way in which the logic function is performed being based upon a value of a function selection signal (SELECT, p. 4) such that for identical data received at the N data inputs and for different values of the function selection signal (SELECT), at least one of polarities of certain internal nodes of the logic circuit are not identical and current consumption of the logic circuit is not identical (see "Function Table", p. 1 and elaboration of same described below). For SELECT = "0", Y=A and for SELECT = "1", Y=B. Therefore, as per the highlighted areas of the table below, corresponding to the Function Table on p. 1 of NS, with identical data inputs, but different function selection signals, the output polarities are different. Further, for high or low output Y, current consumption is –0.4mA and 4mA, respectively.

SELECT	A	B	Output Y

0	0	0	0
0	0	1	0
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over **NS** in view of one having ordinary skill in the art.

Regarding claim 23, the claim is substantially similar to claim 1 and is therefore rejected under similar rationale. NS lacks refreshing the function selection signal at predetermined instants. However, one having ordinary skill in the art knows the purpose of a multiplexer is to select between multiple signals and therefore it is known to refresh the selection signal at predetermined instants (when it is desired for the output to received data from a different one of the inputs) to use the multiplexer according to its function. Therefore, it would have been

obvious to one having ordinary skill in the art at the time the invention was made to modify NS to explicitly refresh the selection signal at predetermined instants. One of ordinary skill in the art would have been motivated to perform such a modification to send the desired input to the output according to the operation of a multiplexer.

Allowable Subject Matter

14. Claims 2-5, 10-22, 24 & 32 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

15. **Review of the most pertinent art to the claims:**

e. U.S. Patent 6,839,847 to Ohki et al. (**Ohki**) discloses a logic circuit for performing a logic function (Fig. 1), and having N data inputs (64-bit plain text and cipher key of 56-bits) and M data outputs (64-bit ciphertext output) (col. 6, lines 41-48), N being at least equal to 2 and M being at least equal to 1, the logic circuit comprising at least one logic gate/circuit for performing the logic function (col. 8, lines 1-14) in at least two different ways (depending on random signal, repetition unit repeats processing) (col. 8, lines 42-60), the way in which the logic function is performed being based upon a value of a function selection signal (col. 8, lines 55-60) such that for identical data received at the N data inputs and for different values of the function selection signal, at least one of polarities of certain internal nodes of the logic circuit are not identical (col. 8, lines 43-49) and current consumption of the logic circuit is not identical (col. 8, lines 58-60). Not that while the random signal affects repeat processing, identical results are

accomplished regarding the output/result of the encryption processing. However, the Ohki disclosure is based on repetition and a such there is nothing to suggest any other than the same logic gates or transistors are to be used; hence Ohki lacks different logic gates or different transistors for performing the logic function each way and lacks the different ways corresponding to different data or electrical paths through the logic gates or transistors.

f. U.S. Patent 6,498,404 to Thuringer et al. describes reversing means/inverter for reversing the data applied to N inputs (Fig. 2, ##6-7), such that a complementary signal is created and hence complementary power consumption is affected. However, while it is inherent that a function selection signal/clock exists in the circuit, Thuringer lacks reversing the output delivered by the gate and lacks the elements of the independent claims in the instant case.

g. U.S. Patent 6,349,318 to Vanstone et al. is cited for teaching supplying a function selection signal (Figs. 1 or 3, #10 & col. 3, lines 3-5) to select a function of an encryption circuit that performs encryption in two different ways (col. 3, lines 3-5). However, the function selection signal is not randomly supplied and the logic function performed (ALU function) is not the same function (the unit 34 performs the function over a finite field and the unit 36 performs the function over integers). The same input, with the exception of the function selection signal (signal 10 in Figs. 1 and 3), would not yield the same output and hence the function is not the same.

h. U.S. Patent 4,968,903 to Smith et al. describes a circuit performing two different logic functions based on a selector signal (see, for example, Fig. 4).

16. However, the following reasons for allowance are given regarding the claims.

i. Regarding claim 2, the prior art relied upon fails to teach or suggest reversing means (inverting) for reversing the data applied to the N inputs of said at least one logic block, and for reversing the data delivered by said at least one logic block based upon the value of a selection signal, in combination with the remaining limitations of the claim.

j. Regarding claim 3, the claim is allowable due to its dependence upon claim 2.

k. Regarding claim 4, the prior art relied upon fails to teach or suggest a logic block comprising a plurality of logic gates for performing a NAND logic function when a selection signal has a first logic value and for performing a NOR logic function when the selection signal has a second logic value, in combination with the remaining limitations of the claim.

l. Regarding claim 5, the prior art of record fails to teach or disclose, either alone or in combination, the selection signal being randomly generated, in combination with the other elements of the claim.

m. Regarding claim 10, the prior art of record fails to teach or disclose, either alone or in combination, wherein the logic function is an encryption function, in combination with the other elements of the claim.

n. Regarding claim 11, the prior art teaches performing a logic function (encryption) in a circuit in two different ways (with unnecessary repetition and without, see Ohki reference), but the prior art relied upon fails to teach or suggest a secured integrated circuit with the feature of an encryption circuit comprising a plurality of encryption

blocks, each encryption block for performing a logic function in at least two different ways, the way in which the logic function is performed being based upon a value of a function selection signal and a random signal generator connected to said plurality of encryption blocks for randomly providing the function selection signal to each encryption block, in combination with the remaining limitations of the claim.

o. Regarding claims 12-22, the claims are allowable based on their dependency upon claim 11.

p. Regarding claim 24, the prior art of record fails to teach or disclose, either alone or in combination, wherein the selection signal is randomly applied to the at least one logic block, in combination with the remaining limitations of the claim.

q. Regarding claim 32, the prior art of record fails to teach or disclose, either alone or in combination, wherein the logic function is an encryption function, in combination with the remaining limitations of the claim.

Conclusion

17. The art made of record and not relied upon is considered pertinent to applicant's disclosure.

Benini is cited for teaching power-managed units where multiple units perform the same function, but use different power requirements to mask the power requirements of a circuit, but does not constitute prior art.

18. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJS

April 9, 2007

David Y. Jung
Primary Examiner

4/11/07